



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,405	08/30/2001	Robert P. Goldman	H0001867 (FSP:114.001US01)	8248
7590	11/10/2004			EXAMINER SHERKAT, AREZOO
Honeywell International Inc. Law Dept. AB2 P.O. Box 2245 Morristown, NJ 07962-9806			ART UNIT 2131	PAPER NUMBER

DATE MAILED: 11/10/2004

3

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	09/943,405	GOLDMAN ET AL.
	Examiner	Art Unit
	Arezoo Sherkat	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 30 August 2001.  
 2a) This action is **FINAL**.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-20 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-20 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 30 August 2001 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date 2.

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

## **DETAILED ACTION**

Claims 1-20 are presented for examination.

### ***Claim Objections***

Claim 17 is objected to because of the following informalities: page 16, line 1, "using to database ..." should read "using a database ...".

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Gleichauf et al., (U.S. Patent No. 6,415,321 and Gleichauf hereinafter).

Regarding claims 1, 3, and 13, Gleichauf discloses a network reference model for use in configuring security software on a computer network, the network reference model comprising:

a database engine providing deduction, a network information database associated with the database engine and providing a central repository for a configuration of hardware and software installed on the network, and a security goal database associated with the database engine and describing uses that the hardware and software installed on the network may support (Col. 5, lines 32-67 and Col. 6, lines 1-67 and Col. 7, lines 1-10).

Regarding claims 4-10, and 14, Gleichauf discloses a configuration tool for use in configuring security software packages on a computer network, the configuration tool comprising:

a description logic database engine, a network information database associated with the description logic database engine and providing a central repository for a configuration of hardware and software installed on the network, a security goal database associated with the description logic database engine and providing security goals describing uses that the hardware and software of the network may support (Col. 5, lines 32-67 and Col. 6, lines 1-67 and Col. 7, lines 1-10);

an event database associated with the description logic database engine and containing events related to the network, wherein the events contained in the event database include possible attacks against the network and benign events that could be confused with the possible attacks (Col. 7, lines 10-25);

a first configuration module coupled to the description logic database engine for configuring intrusion blocking security software packages (i.e., firewalls), a second configuration module coupled to the description logic database engine for configuring intrusion detecting security software packages (i.e., firewalls can detect policy violations and patterns of misuse upon networks to which the Security products are coupled) (Col. 1, lines 20-45),

a system hardening module coupled to the description logic database engine for automating a process of hardening the network, and an audit configuration module coupled to the description logic database engine for probing the network for vulnerabilities, wherein the first configuration module configures the intrusion blocking security software packages based on the configuration of the hardware and software installed on the network and the security goals, wherein the second configuration module configures the intrusion detecting security software packages based on the configuration of the hardware and software installed on the network and the security goals; and wherein the system hardening module is context sensitive (Col. 4, lines 1-67 and Col. 5, lines 1-30).

Regarding claims 11 and 15, Gleichauf discloses a method for configuring a security software package installed on an individual network device, the method comprising:

using active inference in an object-oriented description logic database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device, wherein the individual network device is a member of the class of network devices (Col. 5, lines 15-31); and

configuring the security software package using the one or more security goals, wherein the security software package is selected from the group consisting of an intrusion blocking software package and an intrusion detecting software package (Col. 4, lines 22-67 and Col. 5, lines 1-67 and Col. 6, lines 1-67).

Regarding claims 12 and 16, Gleichauf discloses wherein using active inference further comprises automatically classifying the individual network device based on an IP address, a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification (Col. 4, lines 47-67 and Col. 5, lines 1-14).

Regarding claim 17, Gleichauf discloses a method for configuring a security software package, the method comprising:

defining one or more security policies for a class of network devices, wherein the security software package is a service running on at least one network device of the

class of network devices, using a database engine providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals, using a database engine providing deduction to associate the one or more security goals with the at least one network device, and configuring the security software package on the at least one network device using the one or more security goals (Col. 4, lines 22-67 and Col. 5, lines 1-67 and Col. 6, lines 1-67).

Regarding claims 18-20, Gleichauf discloses a method for configuring security software packages, comprising:

generating a first database containing a configuration of hardware devices and software packages installed on a network, wherein the software packages include the security software packages, generating a second database containing first security goals (Col. 5, lines 32-67 and Col. 6, lines 1-67 and Col. 7, lines 1-10);

defining classes of hardware devices installed on the network, automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine providing deduction (Col. 4, lines 22-67 and Col. 5, lines 1-67 and Col. 6, lines 1-67);

decomposing the first security goals into second security goals for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network, and configuring each of the security software packages using the second security goals (Col. 5, lines 15-31).

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Lermuzeaux et al., (U.S. Patent No. 5,621,889),

Schlossberg et al., (U.S. Publication No. 2002/0066034),

Gleichauf et al., (U.S. Patent No. 6,499,107),

Shieh et al., (U.S. Patent No. 5,278,901),

Antur et al., (U.S. Patent No. 6,212,558),

Cheline et al., (U.S. Publication No. 2003/0041136),

Moriconi et al., (U.S. Publication No. 2001/0007133),

Sciacca, (U.S. Patent No. 6,760,761),

Sherlock et al., (U.S. Publication No. 2002/0093527), and

Rothermel et al., (U.S. Patent No. 6,499,107).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

*A. Sherkat*

Arezoo Sherkat  
Patent Examiner  
Art Unit 2131  
Nov. 04, 2004

*Ayaz Sheikh*  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100